

# Liferay 6.2 integration with Azure AD

Configuration Azure AD default directory

Create a new Application registration

Microsoft Azure

Search resources, services, and docs (G+I)

8

?

😊

DEFAULT DIRECTORY

Home > Default Directory >

liferay-integration-azure-ad

✕

Search (Ctrl+I)

«

🗑️ Delete

🌐 Endpoints

🔍 Preview features

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Essentials

Display name  
liferay-integration-azure-ad

Application (client) ID  
[REDACTED]

Directory (tenant) ID  
[REDACTED]

Object ID  
[REDACTED]

Supported account types  
My organization only


Redirect URIs  
1 web, 0 spa, 0 public client

Application ID URI  
Add an Application ID URI

Managed application in local directory  
liferay-test

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

View API permissions

Documentation

[Microsoft identity platform](#)

[Authentication scenarios](#)

[Authentication libraries](#)


[Code samples](#)

[Microsoft Graph](#)

[Glossary](#)

[Help and Support](#)

Sign in users in 5 minutes



Use our SDKs to sign in users and call APIs in a few steps

View all quickstart guides

Register in authentication a platform configuration

Microsoft Azure

Search resources, services, and docs (G+)

8

?

😊

DEFAULT DIRECTORY

Home > Default Directory > liferay-integration-azure-ad

liferay-integration-azure-ad

Authentication

✕

Search (Ctrl+)

«

Save

Discard

Got feedback?

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart

Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https:// /c/portal/login

Add URI

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

https:// /c/portal/logout

✓

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☒ Access tokens

☒ ID tokens

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

[Help me decide...](#)

Create a secret configuration for the application

Microsoft Azure

Search resources, services, and docs (G+J)

8

?

😊

DEFAULT DIRECTORY

Home > Default Directory > liferay-integration-azure-ad

🔑

liferay-integration-azure-ad | Certificates & secrets

✕

🔍 Search (Ctrl+J)

«

📄 Got feedback?

🏠 Overview

👤 Quickstart

🔧 Integration assistant | Preview

Manage

🏠 Branding

🔄 Authentication

🔑 Certificates & secrets

🔑 Token configuration

🔑 API permissions

🔑 Expose an API

👤 Owners

👤 Roles and administrators | Preview

📄 Manifest

Support + Troubleshooting

🔧 Troubleshooting

👤 New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

📄 Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value
liferay-secret	26-10-2021	Qy9*****

Here are the endpoints to use in liferay

Microsoft Azure Upgrade Search resources, services, and docs (G+/I) DEFAULT DIRECTORY

Home > Default Directory

## Default Directory | App registrations

Azure Active Directory

Overview

- Getting started
- Preview hub
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations**
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security

Monitoring

- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings

+ New registration Endpoints Troubleshooting Download Preview features

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph.

All applications Owned applications Applications from personal account

Start typing a name or Application ID to filter these results

Display name

liferay-integration-azure-ad

### Endpoints

Copy to clipboard

OAuth 2.0 authorization endpoint (v2)	https://login.microsoftonline.com/ /oauth2/v2.0/authorize
OAuth 2.0 token endpoint (v2)	https://login.microsoftonline.com/ /oauth2/v2.0/token
OAuth 2.0 authorization endpoint (v1)	https://login.microsoftonline.com/ /oauth2/authorize
OAuth 2.0 token endpoint (v1)	https://login.microsoftonline.com/ /oauth2/token
OpenID Connect metadata document	https://login.microsoftonline.com/ /v2.0/.well-known/openid-configuration
Microsoft Graph API endpoint	https://graph.microsoft.com
Federation metadata document	https://login.microsoftonline.com/ /federationmetadata/2007-06/federationmetadata.xml
WS-Federation sign-on endpoint	https://login.microsoftonline.com/ /wsfed
SAML-P sign-on endpoint	https://login.microsoftonline.com/ /saml2
SAML-P sign-out endpoint	https://login.microsoftonline.com/ /saml2

Users for this integration is based having email, lastname, firstname the same as in liferay.

Microsoft Azure Upgrade Search resources, services, and docs (G+/J) DEFAULT DIRECTORY

Home > Default Directory > Users > Liferay portal administrator

### Liferay portal administrator | Profile

User

Diagnose and solve problems

Manage

- Profile
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-ins
- Audit logs

Troubleshooting + Support

- New support request

**Liferay portal administrator**  
administrator.portal@...onmicrosoft.com

User Sign-ins

Group memberships

**Identity**

Name	Liferay portal administrator	First name	Administrator	Last name	Portal
User Principal Name	administrator.portal@...onmicrosoft.com	User type	Member		
Object ID		Source	Azure Active Directory		

**Job info**

Job title	Department	Manager
...	...	...
Company name	Employee ID	...
...	...	...

**Settings**

Block sign in	Usage location
No	

**Contact info**

Street address	State or province	Country or region	Office
...	...	...	...
City	ZIP or postal code	Office phone	Mobile phone
...	...	...	...
Email	Alternate email	Proxy address	View more
administrator.portal@...	...		

**Authentication contact info**

Use the [Authentication methods](#) page to manage authentication contact info for a user

## Configuration properties liferay

add the following property in your tomcat installation /opt/tomcat/bin/setenv.sh

**setenv.sh**

-Dcompany-id-properties=true

[graph.microsoft.com](https://graph.microsoft.com) certificate

microsoft.cer

```
-----BEGIN CERTIFICATE-----
MI I INjCCBh6gAwIBAgITMwABX4fknS14INGvvgAAAAFfhzANBgkqhkiG9w0BAQwF
ADBZMQswCQYDVQQGEwJVUzEeMBwGA1UEChMVTWl jcm9zb2Z0IENvcnBvcnF0aW9u
MSowKAYDVQQDEyFNaWNYb3NvZnQgQXplcmUgVExTIElzc3VpbmcgQ0EgMDEwHhcN
MjAwOTE1MTkwMjE3WmcNMjEwOTEwMTkwMjE3WjBqMQswCQYDVQQGEwJVUzELMAKG
A1UECBMVC0ExEDAOBgNVBACTB1JlZG1vbmcQxHjAcBgNVBAoTFU1pY3Jvc29mdCBD
b3Jwb3JhdG1vb3Jlc3VpbmcGA1UEAxMTZ3JhcGubWl jcm9zb2Z0LmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADGgEPADCCAQoCggEBANPGoHShsDsxewJk juZt6fX/L2JKMqq6
NilXNscWsMG4gUYw70u1I75dkEPnyA8+RK+a1+wF3vakxXHjeVMae00FJUW8csui
A1Yahb1pDKG2FMXsPULoTs+1LFziwEWO5olLxvdH9nW/Tx7U8sQ5/eY0S/Z94mx
8oWRMUfSb1JEUaJk15DZxgi7uCPgKvXE9ccVAElBD+x7u3yZe/sG0fOw75WB9igK
91nv2B6CnV9LfkQKvUDK/1383ZtYSay4UovHGLS2QBn/1xPstHS6xxbrOaTZaxMT
lsHDL67AXjpJD9JCtmjKmsD38Y71oeQL5CgAkOvtBTNouqshSUZkmXMCawEAAaOC
A+QwggPgMIIBfQYKKwYBBAHWeQIEAgSCAW0EggFpAwcAdQD2XJQv0XcwIhRUGAgw
lFaO400TGTO/3wwwIavMTvFk4wAAAXSTLpiBAAAEawBGMEQCIFkgmTWMZMAKzHjgo
v+tVY3sgSzfo0b9Hkj14VnQN8caIAiBwHD5cElcHT84UYOczuSLhoUH5dyfkutqB
8cOydlDe6AB2AFzcQ5L+5qtFRLFemtRW5hA3+9X6R9yh5SyXub2xw7KAAABdJMu
mNcAAQDAECwRQIhALcCxn/LHTqBUxorlp2C/Wy9HWFw5mWfby3xaTr2VrbPAiAH
sx6OJYemcy+Wd54rNTfGmZanDPSFHKnmH/baJ7DotAB2AESUZS6w7s6vxEAH2Kj+
KMDa5oK+2MsxtT/TM5a1toGoAAABdJmumJIAAAQDAECwRQIhAIN3a9ZUMIAddsjj
D+5khJpejWVCgMElrJ8heBcA3DwaAiAPnJZ1pPXn26IABgK5PzqIxzeyaSZ8hNEv
CncOM/GuBDAbBgkrBgEEAYI3FQoEDjAMMAoGCCsGAQUFBwMBMDwGCSsGAQQBgjcV
BwQvMC0GJSsGAQQBgjcVCIE91xuB5+tGgoGdLo7QDIfw2hldgbXdUIWf/XUCAWQC
AR0wga4GCCsGAQUFBwEBB1GhMIGeMG0GCCsGAQUFBzAChmFodHRwOi8vd3d3Lm1p
Y3Jvc29mdC5jb20vcGtpb3BzL2NlcnRzL01pY3Jvc29mdCUyMEF6dXJlJTlWExT
JTIwSXNzdWluZyUyMENBjTIwMDElMjAtJTIweHNpZ24uY3J0MC0GCCsGAQUFBzAB
hiFodHRwOi8vb25lb2NzcC5taWNYb3NvZnQuY29tL29jc3AwHwQYDV0ROBBYEFPGE
tncncIF0F/gVJe14zT9BxK8VMA4GA1UdDwEB/wQEAwIESDAeBgNVHREEFzAVghNn
cmFwaC5taWNYb3NvZnQuY29tMGQGA1UdHwRdMFswWabXoFWGU2h0dHA6Ly93d3cu
bWl jcm9zb2Z0LmNvbS9wa2lvcHMvY3J3Sj01pY3Jvc29mdCUyMEF6dXJlJTlWExT
JTIwSXNzdWluZyUyMENBjTIwMDEuY3J3SGYGA1UdIARfMF0wUQYMKwYBBAGCN0yD
fQEBMEEPwYIKwYBBQUHAgEWM2h0dHA6Ly93d3cuY3J3Sj01pY3Jvc29mdCUyMEF6dXJl
cHMvRG9jcy9SZXBvc2l0b3J5Lmh0bTAIBgZngQwBAGIwHwYDV0R0jBBgwFoAUDyBd
16FXlduSzyvQx8J3BM5ygHYwEwYDV0R0lBAwwCgYIKwYBBQUHAgEwdQYyJKoZIhvcN
AQEMBBQADggIBADn6uS0VJ+KnB0j6hSGy4wSNG6EBHOMqd+IWLByrTJpoSokRvR+F
Dr3eP6oDBAocDZ5Fxm1rZwO3GJD0UZpwoH3WQ8mIvyggaf1d7B2uJVDDehEf1U6C/
AQAhf5utTcvVVJ16oKloDwic7cMK4oMhQAfZ6nWoxsgVKNRiCAJIhy3DFQkTOuX7
kYfbga0DJeR9EMst9EoSSp8859ygr4HJGy03A7H4F45w/OJgSRckSE5gV4x1DaRx
ar3X0tnbm+htfsHk1z29J1jbs1QGUAiQRGLZ7dSZAIO0/94d59N8ZcUoelIRsYS
0liGFJhUyA+LTVbrsXiDbQrw9Ug2ZK2FylQ+weq9hSK7dMefNhQSeNnJruT244h4
F+UuhKrx66QP4RhAcEkmSqUfpzMxfqrnmdHY3kxoQQZo+4/FRjNn9GT1/SC0e4EC
71wMjmxJbVnAfonwUVXxRkpBGMsUeQeF2ln1/66S4GV2KKohAqGV2cEsmP9R/gJn
sweup2Y2PJx4ke3rfou3wC7kFunHe6s8k+Mw7/8Vgl0UAvslkiD46Elg0e/mko8n
7rABZ+E/Stmt7V+P0uhWYRULVcjYLU0pi2N18KXov3HxZy1NfBldihjQl1f0yt4Zy
Y1N4nniJrWqv5HAQkM1/06uX+NZ0ExAt6muFxxQYSp1QraEgk4PUxX1S
-----END CERTIFICATE-----
```

[login.microsoftonline.com](https://login.microsoftonline.com/certificate) certificate

#### azure.cer

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWzJWZHHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDEXdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAEfw0wNjExMTAwMDAwMDBaFw0zMTEwMTAwMDAwMDBaMGExCzAJBgNVBAYTA1VT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMTIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTToleqUKKPC3eQyaKl7hL0l1sB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/S10fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYmq1lGNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
Tl9sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSjletX+jkM0vJwIDAQABO2MwyTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNvbr
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNvbrTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfTfrgTleXkIoYQY/Esr
hMatudXH/vTBH1jLuG2cenTnmCmrEbXjckChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRbc4L0na4UU+Krk2U886UAb3Lujev0ls
YSEYlQSteDwsOoBrp+uvFRTP2InBuThs4pFsiV9kuXclVzDAGySj4dZp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpG0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

## Add the microsoft following certificates to java keystore

#### java keystore certificates

```
cd $(readlink -f /usr/bin/javac | sed "s:/bin/javac::")
cd jre/lib/security/
# the password is changeit
keytool -import -alias graph.microsoft.com -keystore cacerts -file /opt/liferay/microsoft.cer
keytool -import -alias login.microsoftonline.com -keystore cacerts -file /opt/liferay/azure-ad.cer
```

## Install the following liferay OpenID plugin

Beheren Installeren

## Installeren

☒ Bestand uploaden (JAR, LPKG of WAR-bestand)

Bestand kiezen Geen bestand gekozen

☐ URL

Installeren



oidc-hook-0.5.3.war

Add the following values in **portal-ext.properties**



## porta-ext.properties

```
#open id azure active directory
openidconnect.enableOpenIDConnect=true
openidconnect.token-location=https://login.microsoftonline.com/{TENANT-APP-ID}/oauth2/v2.0/token
openidconnect.authorization-location=https://login.microsoftonline.com/{TENANT-APP-ID}/oauth2/v2.0/authorize
openidconnect.profile-uri=https://graph.microsoft.com/oidc/userinfo
openidconnect.user-membership-location=https://graph.microsoft.com/v1.0/me/memberOf
openidconnect.issuer=https://login.microsoftonline.com/{TENANT-APP-ID}/v2.0
openidconnect.client-id={APPID-APP-REGISTRATION}
openidconnect.secret={SECRET-CONFIGURED-APP-REGISTRATION}
openidconnect.scope=openid profile email
openidconnect.provider=azure-default
openidconnect.sso-logout-uri=https://login.microsoftonline.com/{TENANT-APP-ID}/oauth2/v2.0/logout
```